

Chapter V

Privacy and Trust in Online Interactions

Leszek Lilien

Western Michigan University, USA

Bharat Bhargava

Purdue University, USA

ABSTRACT

Any interaction—from a simple transaction to a complex collaboration—requires an adequate level of trust between interacting parties. Trust includes a conviction that one's privacy is protected by the other partner. This is as true in online transactions as in social systems. The recognition of the importance of privacy is growing since privacy guarantees are absolutely essential for realizing the goal of pervasive computing. This chapter presents the role of trust and privacy in interactions, emphasizing their interplay. In particular, it shows how one's degree of privacy can be traded for a gain in the level of trust perceived by the interaction partner. After a brief overview of related research, the idea and mechanisms of trading privacy for trust are explored. Conclusions and future trends in dealing with privacy and trust problems complement the chapter.

INTRODUCTION

Any interaction—from a simple transaction to a complex collaboration—can be successful only if an adequate level of trust exists between interacting entities. One of the more important

components of trust of an entity in its interaction partner is its reliance that the partner is both willing and able to protect entity's privacy. This is as true in the cyberspace as in social systems.

The need for privacy is broadly recognized by individuals, businesses, the government, the

computer industry, and academic researchers. Examples are shown in Table 1. The growing recognition of the importance of privacy is motivated not only by users' sensitivity about their personal data. Other factors include business losses due to privacy violations, and enactments of federal and state privacy laws. Even more important, the quest for the promised land of pervasive computing will fail if adequate privacy guarantees are not provided.

The role of trust and privacy is fundamental in social systems as well as in computing environments. The objective of this chapter is presenting this role in online interactions, emphasizing the close relationship between trust and privacy. In particular, we show how one's degree of privacy can be traded for a gain in the level of trust perceived by one's interaction partner.

We begin with a brief overview in the next section, presenting the background for research on

trust, privacy, and related issues. First, we define trust and privacy, and then discuss their fundamental characteristics. Selecting the most relevant aspects of trust and privacy to be employed in a given application and computing environment is in and by itself a significant challenge. The reason is that both trust and privacy are very complex, multifaceted concepts.

Privacy and trust in computing environments are as closely related and as interesting in various aspects of their interplay as they are in social systems (Bhargava, Lilien, Rosenthal, & Winslett, 2004). On the one hand, a high level of trust can be very advantageous. For example, an online seller might reward a highly trusted customer with special benefits, such as discounted prices and better quality of services. To gain trust, a customer can reveal private digital credentials—certificates, recommendations, or past interaction histories. On the other hand, a mere

Table 1. Recognition of the need for privacy by different entities

<p>Recognition of the need for privacy by individuals (Cranor, Reagle, & Ackerman, 1999)</p> <ul style="list-style-type: none"> • 99% unwilling to reveal their SSN • 18% unwilling to reveal their favorite TV show
<p>Recognition of the need for privacy by businesses</p> <ul style="list-style-type: none"> • Online consumers worrying about revealing personal data held back \$15 billion in online revenue in 2001 (Kelley, 2001)
<p>Recognition of the need for privacy by the federal government</p> <ul style="list-style-type: none"> • Privacy Act of 1974 for federal agencies (Privacy Act, 2004) • Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Summary HIPAA, 2003; Mercuri, 2004)
<p>Recognition of the need for privacy by computer industry research (examples)</p> <ul style="list-style-type: none"> • IBM—incl. Privacy Research Institute (IBM Privacy, 2007) • Topics include: pseudonymity for e-commerce, EPA, and EPAL—enterprise privacy architecture and language, RFID privacy, privacy-preserving video surveillance, federated identity management (for enterprise federations), privacy-preserving data mining and privacy-preserving mining of association rules, hippocratic (privacy-preserving) databases, online privacy monitoring • Microsoft Research—including Trustworthy Computing Initiative (Trustworthy Computing, 2003) • The biggest research challenges: reliability/security/privacy/business Integrity • Topics include: DRM—digital rights management (incl. watermarking surviving photo editing attacks), software rights protection, intellectual property and content protection, database privacy and privacy-preserving data mining, anonymous e-cash, anti-spyware
<p>Recognition of the need for privacy by academic researchers (examples)</p> <ul style="list-style-type: none"> • Trust negotiation with controlled release of private credentials, privacy-trust tradeoff • Trust negotiation languages • Privacy metrics • Anonymity and k-anonymity • Privacy-preserving data mining and privacy-preserving database testing • Privacy-preserving data dissemination • Preserving location privacy in pervasive computing, and privacy-preserving location-based routing and services in networks • Trust negotiation with controlled release of private credentials • Genomic privacy

36 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/privacy-trust-online-interactions/27732

Related Content

Customer Engagement: Storytelling and the UK's Leading Retailers

Peter Jones and Daphne Comfort (2020). *Handbook of Research on Contemporary Consumerism* (pp. 57-71). www.irma-international.org/chapter/customer-engagement/238533

Identity-Based Consumer Behaviour, Self-Congruity, and Retailer-Consumer Relationships: A Literature Review

Isabella Maggioni (2014). *Handbook of Research on Retailer-Consumer Relationship Development* (pp. 13-26). www.irma-international.org/chapter/identity-based-consumer-behaviour-self-congruity-and-retailer-consumer-relationships/109680

A Framework for E-Service Implementation in the Developing Countries

H. S. Hassan, E. Shehab and J. Peppard (2013). *Managing Customer Trust, Satisfaction, and Loyalty through Information Communication Technologies* (pp. 54-67). www.irma-international.org/chapter/framework-service-implementation-developing-countries/74548

Customer Acquisition Management Strategies

(2015). *Customer Relationship Management Strategies in the Digital Era* (pp. 219-243). www.irma-international.org/chapter/customer-acquisition-management-strategies/126394

A Knowledge Management Approach to Marketing and the Advent of Customer Knowledge Management

Samiha Mjahed and Abdelfattah Triki (2012). *Customer-Centric Knowledge Management: Concepts and Applications* (pp. 264-284). www.irma-international.org/chapter/knowledge-management-approach-marketing-advent/58038